FOR ATTORNEYS, FIDUCIARIES AND FIRM IT

Security & privacy overview

Last reviewed 5 November 2026.

In one paragraph

FiduKit is browser software that turns bank and brokerage statement PDFs into a California GC-400 accounting. The statements are read and the accounting is built **inside the user's browser, on the user's computer**. FiduKit's servers handle only sign-in and payment, and their database has no place to store a statement, a transaction, a balance or an account number.

What never leaves the browser

- **Statement PDFs, registers, transactions, balances, categories and account numbers.** Statements are read with PDF.js (Mozilla's open-source PDF library) in a Web Worker, a background thread of the page. Categorizing, balancing and filling the court forms happen in the same place. The finished packet is written to your Downloads folder.
- **Where the work is saved:** in the browser's own storage (IndexedDB) on that computer, including the original statement PDFs, so the packet can attach them. FiduKit does not add its own encryption to that storage. It is protected by the computer's sign-in and disk encryption, so we recommend full-disk encryption (BitLocker or FileVault) and a browser profile that is not shared.
- **No analytics and no error reporting service in the app.** An error is written to the browser's own console with figures, email addresses and file names removed; nothing is sent.

Exactly what the server stores

The database (Cloudflare D1) has these tables, and nothing else:

TABLE	WHAT IT HOLDS
Accounts	Email address, name, a password hash (or your Google account ID instead), when the account was created, last sign-in date, when the email address was confirmed, and a counter that lets "Sign out of all devices" end every session at once.
Email-link tokens	For confirming an address, resetting a password or changing an email: only a SHA-256 hash of each link. Links expire after 15 minutes (24 hours for the sign-up confirmation).
Purchases	Polar's order number, amount, status and dates, a random reference your browser generated for the accounting, and a signed unlock token. No case name.
Payment events	Polar's event IDs and types, so a payment notice is never applied twice.
Administration	FiduKit's own two-factor secret (encrypted) and a record of any access we grant or revoke by hand.
Reserved, unused	Tables for a deadline-reminder feature (a case label, a period-end date and a due date). That feature is not available, and the app writes nothing to them.

An automated test reads the database schema and fails the build if any table or column outside this list appears. Sessions are not stored in the database: they are signed cookies (below). Rate-limit counters are kept briefly, under a keyed hash rather than a raw email or IP address.

Check it yourself: the Content-Security-Policy

The app at `app.fidukit.com` is served with this policy, fixed in the deployed files (not built from settings):

```
default-src 'self'; script-src 'self' 'wasm-unsafe-eval'; style-src 'self' 'unsafe-inline'; img-src 'self' blob: data:;
font-src 'self'; connect-src 'self'; worker-src 'self' blob:; manifest-src 'self'; frame-ancestors 'none'; base-uri
'self'; form-action 'self'; object-src 'none'
```

`connect-src 'self'` means the browser itself refuses any request from the page, or from its background workers, to anywhere except `app.fidukit.com`. No analytics host, no payment host and no AI service is on the list. Checkout leaves the app by a normal page navigation to Polar.

1. Open the app, press `F12`, choose the **Network** tab and clear it.
2. Add statement PDFs and work the accounting through to the download.
3. Every request listed goes to `app.fidukit.com`: the app's own files, blank court forms, PDF.js font maps, and the sign-in and purchase checks, which carry at most a random accounting reference and never a figure. Click the page request and read the `Content-Security-Policy` response header to see the policy above.

Encryption, passwords and sign-in

- **Connections:** HTTPS only, with HTTP Strict Transport Security on the app, the site and the API.
- **Backup file (.cpx):** encrypted in the browser before it is saved, with AES-256-GCM. The key comes from your passphrase through PBKDF2-SHA-256 with 600,000 iterations and a random 16-byte salt. We never see the passphrase and cannot recover a lost one. A tampered file fails to open.
- **Passwords:** never stored. Each is first keyed with HMAC-SHA-256 under a secret "pepper" held in the server's secret store, never in the database, then hashed with PBKDF2-HMAC-SHA-256 (100,000 iterations, a random 16-byte salt). Sign-in, sign-up and password-reset attempts are rate-limited.
- **Google sign-in:** OAuth with PKCE. We keep your email, name and Google account ID, and no Google access token.
- **Session cookie:** `__Host-cp_session`, marked `HttpOnly`, `Secure` and `SameSite=Lax`, limited to `app.fidukit.com`. It lasts 30 days, renews with use, and ends 90 days after sign-in at the latest. Every request that changes something also carries an anti-forgery (CSRF) token held only in the page's memory.

Payments

Payment is taken by **Polar**, the merchant of record, on Polar's own checkout page. Card details go to Polar and never reach FiduKit's servers. We send Polar your email address, your account ID and the random accounting reference, and we keep Polar's order number, the amount and the status. Polar never sees a statement, a transaction or a conservatee's name.

Account numbers on court forms

On the GC-400 forms FiduKit fills, account numbers print as the last four digits only (California Rules of Court, rule 1.201(a)(2)), for example `··4321`. Check, reference and trace numbers are left as printed. The statements attached under Probate Code §2620(c) are your bank's own PDFs and usually show full account numbers; the app says so and points you to your court's rules. Your working papers (CSV and Excel) and the backup file are your own records and are not masked.

No AI in the data path

Statements are read and transactions categorized by deterministic code: a rules engine that gives the same answer every time and states its reason for each flag. FiduKit uses no AI model or AI service, so client data cannot reach one.

Hosting, email, logs and deletion

- **Hosting:** Cloudflare (Pages for the site and app, Workers for the API, D1 for the database). Like any host, Cloudflare receives IP addresses and basic request data.
- **Email:** sent through Resend: sign-up and email-change confirmations, password resets, purchase confirmations and account notices. Resend receives the address and the message.
- **Server logs:** event names, an account ID, a keyed hash of the email address and the outcome. Never a password, a statement or a figure.
- **Deleting an account** removes the account, its sign-in links and its sessions at once. Purchase records are kept for tax and accounting, unlinked from your name. Work in your browser is untouched; delete it there.
- FiduKit is operated from the United States and Pakistan and is intended for users in the United States.

What we don't offer

We have **no SOC 2 report, no ISO 27001 certification and no third-party penetration test**, and no single sign-on (SAML) or on-premises version. By design, the client data a firm worries about never reaches us. We are glad to answer a security questionnaire by email.

Security questions and reports

Email support@fidukit.com. We answer within one business day. Please describe what you see and never attach client data. Post: FiduKit, 8 The Green #10137, Dover, DE 19901, United States. More on privacy: privacy and security and the privacy policy.

FiduKit is document-preparation software, not a law firm: we give no legal advice and file nothing with any court. You review, sign and file your own accounting (California GC-400 series; Probate Code §2620). Not affiliated with or endorsed by the Judicial Council or any court — consult an attorney about your case.